UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,638	12/12/2003	Christele Bouchat	Q78553	1619

23373 7590 12/23/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
RAHIM, MONJUR	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,638	BOUCHAT ET AL.	
	Examiner	Art Unit	
	MONJOUR RAHIM	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment and argument field on ***09/19/2008***.

2. ***Claims 1-11*** are currently pending and ***claims 1,*** *7* and ***8*** are independent claims.

3. ***Claim 12*** is cancelled.

4. Specification Objection has been withdrawn.

Information Disclosure Statement

5. The Information Disclosure Statement (IDS) submitted on 12/12/2003 and 04/13/2004 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the IDS statement is being considered by the examiner.

Priority

6. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 02293184 (EPO), filed on 12/20/2002.

Drawings

7. The drawings filed on 12/12/2003 are accepted by the examiner.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable being anticipated by Medvinsky et al. (US Pub No. 2001/0047484 A1), hereinafter Medvinsky and in view of Slaughter et al. (US Patent No. 6898618), hereinafter Slaughter.

As per ***claim 1***, Medvinsky discloses:

- comprising in a session message of said protocol a user identification that uniquely identifies said user said session parameter and said generated credential (Medvinsky, paragraph [0011], "A "Key Distribution Center" ("KDC") is a network service that supplies tickets and temporary session keys; or an instance of that service or the host on which it runs. The KDC services both initial ticket and ticket-granting ticket (TGT) requests. The initial ticket portion is sometimes referred to as "authentication server" (or "authentication service"). The ticket-granting ticket portion is sometimes referred to as the ticket-granting server (or "ticket granting service")");

-forwarding said session message by said user equipment to said authentication device (AUTH) (Medvinsky, paragraph [0012], "DHCP" defines the protocol exchanges for a client to obtain its IP address and network configuration information from a DHCP Server. Kerberos V5 defines the protocol and message exchanges to mutually authenticate two parties");

- upon reception by said authentication device (AUTH) of said session message verifying said received credential with a generated verification credential based upon said received session parameter and said user password being associated to said received user identification (and thereby providing said authentication for said user (Medvinsky, paragraph [0096], " AP_REQ contains the Kerberos ticket for the DHCP server and also contains information needed by the DHCP server to authenticate the client. After verifying the AP_REQ and decrypting the Kerberos ticket, the DHCP server is able to extract a session key which it now shares with the DHCP client").

Medvinsky does not explicitly teach - **generating by said user equipment a credential based upon a user password,** however in a relevant art Slaughter discloses (Slaughter, col 54, lines 20-26, "The service may then authenticate the credential when received in a message from the client. In one embodiment, the service may send the credential when first received to the same authentication service used by the client to generate the credentials. Thus, the issuing and embedding of credentials in leasing messages may be used to provide a secure leasing environment and (Slaughter, col 62, lines 4-12, "For services that do not restrict access, a gate may be built without an authentication credential or with an "empty" authentication credential. The gates for such services may not send an authentication credential with each message, or may

send an empty credential. The authentication service is one example of a service that may not restrict access. Other services may require a user and password pair.

This gives the user a quick and easy way to create credentials. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to use Slaughter's invention modify Medvinsky so that the authentication process gets harder to break in by the unwanted guest.

As per ***claim 2***, claim 1 is incorporated and Medvinsky discloses:

- ***characterized in that said method further comprises also determining according to predefined rules and conditions an acceptance of said received session parameter*** (Medvinsky, paragraph [0018] One embodiment takes a unique approach to providing authentication support for dynamic parameter assignment protocols using security protocols. Among other aspects, substantial flexibility is gained by decoupling parameter assignment exchanges from security exchanges").

As per ***claim 3*** claim 1 is incorporated and Medvinsky discloses:

-The method to provide an authentication for a user according to claim 1, characterized in that said protocol is a Dynamic Host Configuration Protocol (Medvinsky, Abstract, A method for an un-initialized client to obtain credentials from a server which are then used to provide authenticated exchange for network configuration parameter assignment. The obtained credentials can be applied to an authentication option when a dynamic host configuration protocol DHCP is being used for address assignment").

As per ***claim 4***, claim 1 is incorporated and Medvinsky discloses:

- The method to provide an authentication for a user according to claim 1, characterized in that said session message is a Discover message of a Dynamic Host Configuration Protocol (Medvinsky, paragraph [0010], "A "DHCP" client" is an internet host using DHCP to obtain configuration parameters such as a network address. A "DHCP server" is an internet host that returns configuration parameters to DHCP clients. A "ticket" is a Kerberos

term for a record that helps a client authenticate itself to a server. A ticket contains the client's identity; a session key, a timestamp, and other information, all sealed using the server's secret key. A ticket serves to authenticate a client when presented along with a fresh authenticator"), where "session key", "timestamp" are the parameter in the session (message)").

As per ***claim 5***, claim 4 is incorporated and Medvinsky discloses:

- The method to provide an authentication for a user according to claim 4, characterized in that said user identification said session parameter and said generated credential being included as a predefined Option in an Option field of said Discover message (Medvinsky, paragraph [0015], "Kerberos is a secure key management mechanism that is based on a trusted 3.sup.rd party, the KDC. In Kerberos a client performs mutual authentication with the KDC and in the process obtains credentials (e.g., a Kerberos ticket) that it needs for authentication to an application server (e.g., the DHCP server). The client can then use the Kerberos ticket to perform mutual authentication with the DHCP server and to establish a shared session key that would be used for subsequent message authentication").

As per ***claim 6***, claim 1 is incorporated and Medvinsky discloses:

- The method to provide an authentication for a user according to claim 1 characterized in that said session parameter is a session identifier that uniquely identifies said session that is actual being established (Medvinsky, paragraph [0010], "A ticket contains the client's identity, a session key, a timestamp, and other information, all sealed using the server's secret key. A ticket serves to authenticate a client when presented along with a fresh authenticator"), where "session key" is the unique identifier of a session, as claimed.

As per ***claim 7***, Medvinsky discloses:

- a first generator to generate a credential based upon a user password being associated to said user and a session parameter being determined by said user equipment for said session which is actual being established (Medvinsky, paragraph [0010], "A ticket contains the client's identity, a session key, a timestamp, and other information, all sealed using the server's secret key. A ticket serves to authenticate a client when presented along with a fresh

authenticator"), where "ticket" is the credential, which is generated to function uniqueness of authenticity, as claimed.

- a second generator to comprise in a session message of said protocol a user identification uniquely identifying said user said session parameter and said generated credential and to forward said session message to said authentication device in order to enable thereby said authentication device ,upon reception of said session message to verify said received with a generated verification credential based upon said received session parameter and said user password that is associated to said received user identification and to provide thereby said authentication for said user (Medvinsky, paragraph [0020], "An authentication and parameter exchange sequence can be initiated by a DCHP-client broadcast or other appropriate Kerberos message. The proxy, which can be invisible to the client … authentication and parameter assignment exchanges (e.g. including an IP address assignment) can be conducted in a largely conventional manner"), where "broadcasting session message" with session parameter to authenticate, as claimed.

As per ***claim 8***, Medvinsky discloses:

- a third generator to generate a verification credential based upon a received session parameter and based upon a user password that is associated to a received user identification and to provide said verification credential to a verifier (Medvinsky, paragraph [0091], "The client, upon receiving a broadcast response having a link layer destination address as its hardware address and a network layer address as the broadcast address, must verify that the hardware address in the ticket corresponds to its link layer address. Upon receiving a TGS_REP (or an AS_REP with the application server ticket) from the proxy, the client will have enough information to securely communicate with the application server (the DHCP-server in this case), as specified in the following section");

- said verifier coupled to said third generator to verify said verification credential against a received credential and to provide thereby said authentication for said user (Medvinsky, paragraph [00502], "This can be initiated as shown by block 920 in which an authenticated first message from the client to the server is sent as part of the authenticated

address assignment protocol. Thus, the server can utilize the credentials to authenticate this first message received from the client, as illustrated by block 924");

- said received user identification said received session parameter and said received credential being comprised by said user equipment in a session message of said protocol (Medvinsky, paragraph [0045], "As with system 100 of FIG. 1, the substantial decoupling present in system 200 (FIG. 2) enables the authentication phase to be conducted in a manner largely consistent with that of a conventional Kerberos key management exchange. That is, a client gets a ticket granting ticket ("TGT") by contacting an authentication server within a KDC using As Request and Reply messages (see FIG. 5). The client then contacts a Ticket Granting Server in a KDC to get a server ticket using TGS_REQ and TGS_REP messages (which ticket permits initiation of the parameter exchange phase). It is also possible for a client to obtain a DHCP server ticket directly with the AS Request/Reply exchange, and without the use of the TGT");

- said credential being generated by said user equipment based upon said user password that is uniquely associated to said user and said session parameter that is determined by said user equipment for said session which is actual being established (Medvinsky, paragraph [0103], [0104], "The above examples could also be modified such that DHCPclients would not require any additional configuration information other than a password or a key (and a public key certificate if PKINIT is useed. In the above examples, the Kerberos session key is used directly as an HMAC key to authenticate DHCP message. Standard security practice, however, is to use different keys for different purposes. Thus, the Kerberos session key is used to encrypt a part of an AP_REQ message");

- said session message being forwarded by said user equipment to said authentication device (Medvinsky, paragraph [0079], "The client sends TGS Request for a principal name `dhcpsrvr` with the realm found in the TGT to the proxy").

As per ***claim 9***, claim 8 is incorporated and Medvinsky discloses:

- The authentication device according to claim 8, characterized in that said authentication device is at least partly included in a network access provider (Medvinsky,

paragraph [0043], "Customized hardware might also be utilized and/or particular elements might be implemented in hardware, software (including so-called "portable software," such as applets) or both. Further, while connection to other computing devices such as network input/output devices (not shown) may be employed, it is to be understood that wired, wireless, modem and/or other connection or connections to other computing devices might also be utilized").

As per ***claim 10***, claim 6 is incorporated and Medvinsky discloses:

- Telecommunication network to provide an authentication for a user, characterized in that said telecommunication network comprises a user equipment according to claim (Medvinsky, Abstract, "A method for an un-initialized client to obtain credentials from a server which are then used to provide authenticated exchange for network configuration parameter assignment. The obtained credentials can be applied to an authentication option when a dynamic host configuration protocol DHCP is being used for address assignment"), where computer network is capable of carry data, video and voice, as claimed.

As per ***claim 11,*** claim 8 is incorporated and Medvinsky discloses:

- An authentication device according to claim 7(Medvinsky, paragraph [0043], "Operating system utilization will also vary depending on the particular host devices and/or process types (e.g. computer, appliance, portable device, etc").

Conclusion

9 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see form "PTO-892 Notice of Reference Cited").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monjour Rahim whose telephone number is (571)270-3890. The examiner can normally be reached on 5:30 AM -3:30 PM (Mo-Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571)272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (in USA or CANADA) or 571-272-1000.

/Monjour Rahim/
Patent Examiner
Art Unit: 2134
Date: 12/19/2008

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434